Mathematician Jens Fankhänel

A legally secure, digital procedure for confirming parcel acceptance

2nd edition, 3rd July 2025

Mathematician Jens Fankhänel

A legally secure, digital procedure for confirming parcel acceptance

2nd edition, 3rd July 2025

Contents

1 Introduction

Parcel services in the Federal Republic of Germany now only have the delivery of their parcels confirmed by signature on a tablet computer. However, we are convinced that this procedure is not legally secure.
Nevertheless, this very insecure procedure has unfortunately become increasingly widespread. Shipping companies are also having the delivery of their freight confirmed by a signature on a tablet computer. In our experience, it has even happened in public administration that a citizen has been presented with a document to sign on a tablet computer.
In order to make contracts more secure again, the author presents an alternative electronic procedure for signing. A conventional signature, which consists of a handwritten name, should never be drawn on an electronic device. This article shows that a numerical code is sufficient to prove that a certain citizen has signed a certain document. Simply by entering a numerical code, the electronic signature is complete.
Conventional signatures only ever belong on a sheet of paper! The authorities and companies should make a note of this.

2 Explanation of the principle

Each package customer generates a key pair using the well-known RSA method. The customer's public key is stored on a server. Only the customer knows the private key. The customer encrypts the parcel number with his private key and thus receives the numerical code he needs to confirm acceptance of the parcel. Anyone who knows this confirmation code can decrypt it using the customer's public key. If the decryption generates the parcel number again, then the confirmation code was correct.
In particular, the following is proven: Whoever knew the confirmation code for the parcel number must have the private key that belongs to the customer's public key. This is generally only the customer themselves, provided they have not passed on their private key and their private key has not been stolen. This ensures that the customer has signed. The process is even more secure for the parcel service than a conventional signature, which can sometimes be forged.

3 The details

3.1 Storage of the public keys

The public keys of all parcel customers must be stored on the server of an independent organization.
It would be perfectly safe to store the public key on the customer's homepage. But not every parcel customer has their own homepage. Therefore, the public keys of all parcel customers should be managed by an independent organization.
A customer should be able to change their key pair if they no longer consider it secure. In this case, the server should store all of the customer's previous public keys with the respective period of validity. It can then be confirmed that a parcel was accepted when a different key pair was still valid.

3.2 Acceleration of parcel delivery

If the customer uses a private key with more than 2,000 decimal places, then RSA encryption is very secure by today's standards. But the encryption generates a confirmation code that is itself more than 2,000 decimal places long. If every customer were to enter more than 2,000 digits by hand, there could be considerable delays in parcel delivery.
To speed up parcel delivery, customers should save their confirmation code on a USB stick. Before each acceptance of a parcel, a short session on the home computer is necessary to save one or more confirmation codes on the stick.
When the parcel carrier arrives, the customer plugs the stick into a portable computer belonging to the parcel service. The computer reads the stored confirmation codes.
A rewritable chip card could also be used as an alternative to the USB stick. Signing with a chip card would feel like paying with a debit or credit card. On the other hand, writing devices for chip cards are not yet widespread.

4 From the parcel number to the document number

So far, the procedure for secure signing has only been explained for the parcels of a single parcel service. However, the procedure can be used for signing all kinds of documents. It is therefore advisable to make the procedure future-proof for signing very different documents.
With 50-digit numbers, all documents that are to be signed anywhere in the world in the next 500 years can be clearly identified. The package number should be at the very end of the 50-digit document number. A country code should be at the front of the document number. An industry code and a number for each parcel service can also be included in the document number. Places that are not yet required are simply filled with zeros.
The 50-digit document number should therefore be encrypted instead of the parcel number. After decryption, the 50-digit document number, which also contains the parcel number, is returned. Otherwise, the procedure remains the same as explained in chapters 2 and 3.

Bibliography

[1] R.L. Rivest, A. Shamir, and L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; URL: http://people.csail.mit.edu/rivest/Rsapaper.pdf

A Tips for saving paper

Apparently, someone wanted to save paper when parcel services started having their parcels delivered by having them signed for on a tablet computer. But you can save a lot more paper.

A.1 Catalogs

Printed product catalogs are no longer needed. This is because almost all customers in industrialized countries prefer to order online rather than by phone. If you visit a retailer's website, you can easily check which goods are currently available. The Internet provides a lot of additional information about the goods, not all of which can be printed in catalogs.

A.2 Newspapers and magazines

Newspapers and magazines no longer need to be printed in industrialized countries because they can be read on the Internet. Crossword puzzles can be printed out, which would use much less paper than printing an entire magazine. Or crossword puzzles could be made interactive (to be filled in on the computer). Magazines might have to hire a few programmers for this, which would create jobs.

A.3 Telephone directories

In industrialized countries, telephone directories only need to be printed in very small numbers for the elderly and disabled and for people who do not have an Internet connection. Almost all people living in highly developed countries look up the phone numbers they need on the Internet.